



A remote MCP server that lets Claude query and operate the ServiceNow instances the customer registers and controls. This datasheet summarizes security controls and data handling for procurement and IT teams.

Controls

Encrypted credentials

Each instance credential is encrypted at rest with Fernet (AES-128-CBC with HMAC), using a master key that does not live in the database. They are never shown in the panel or in responses.

Exportable audit trail

Every execution is logged: tool, instance, user, date, result and a payload summary without credentials. Export it to CSV.

Production confirmation

Instances flagged as production ask for explicit confirmation before any write.

OAuth 2.1 with PKCE

Claude connects through a standard OAuth flow with PKCE and dynamic client registration. Tokens expire and can be revoked at any time.

IP allowlist

The MCP endpoint can be restricted to authorized addresses or ranges, with an expiry date.

Least privilege

The technical user only has the roles you grant it in ServiceNow. We recommend starting on development or a PDI.

Data stored

Panel account	Email, password hash (bcrypt), role, creation date and last login.
Instances	Alias, URL, technical user and encrypted credential.
OAuth authorization	Registered clients, access and refresh tokens, scopes and source IP.
Audit	Tool, instance, user, date, result and a payload summary without credentials.
Working memory	Only the observations the user or the assistant explicitly save.
Cache	Table metadata and public ServiceNow documentation, with expiry.

What is not stored

- The content of conversations with the assistant.
- ServiceNow records returned by a query, unless the user saves them as an observation.
- No data is used for advertising, profiling or model training.

ServiceNow permissions

The technical user needs the admin role or, at minimum, rest_api_explorer plus the x_mcp_bridge.executor and x_mcp_bridge.script_runner roles once the bridge is installed.

Infrastructure and operations

- HTTPS-only traffic.
- Panel with CSP, HSTS, X-Frame-Options and CSRF protection.
- PostgreSQL database under the control of OPTIMO TECH S.A.S.
- Instances unused for 30 days are invalidated and must be revalidated.
- Access, correction or deletion requests handled within 30 days.

